



IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Applicants: **Young-Sook LIM, Kyung-Hee KANG, Seung-Jae LEE**

Case: **KT-2 (KTP/0/2101)**

Serial No.: **09/774,285**

Filed: **January 30, 2001**

Group Art Unit: **2182**

Confirmation No.: **2529**

Examiner:

Title: **METHOD OF PROVIDING TIME STAMPING SERVICE FOR SETTING
CLIENT'S SYSTEM CLOCK**

COMMISSIONER FOR PATENTS
Washington, D. C. 20231

S I R:

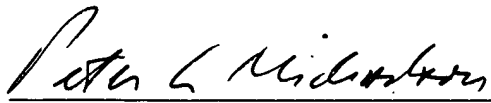
SUBMISSION OF PRIORITY DOCUMENT

In connection with the above-captioned application, applicants enclose the following priority document (together with English translation of certification page) to support the claim to priority:

Korean Appl. No. 68897,
filed November 20, 2000.

Respectfully submitted,

June 19, 2001


Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671



MICHAELSON & WALLACE
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **June 20, 2001** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to the Commissioner for Patents, Washington, D.C. 20231.

Robert L. Michaelson

Signature

30,090

Reg. No.

(k2prior:2/ka)



CERTIFIED COPY OF PRIORITY DOCUMENT

대한민국 특허청 KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Industrial
Property Office.

출원번호 : 특허출원 2000년 제 68897 호
Application Number

출원년월일 : 2000년 11월 20일
Date of Application

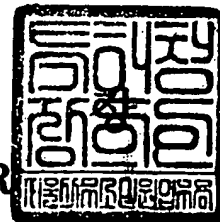
출원인 : 한국전기통신공사
Applicant(s)



2001 01 08
년 월 일

특 허 청

COMMISSIONER





KOREAN INDUSTRIAL PROPERTY OFFICE

This is to certify that the following application annexed hereto is a true copy
from the records of the Korean Industrial Property Office.

Application Number : 2000 Patent Application 68897

Date of Application : November 20, 2000

Applicant(s) : Korea Telecom

On this 8th day of January 2001

COMMISSIONER(Seal)

Application: 09/774,285
Docket No.: KT-2(KTP/0/2101)
Call: Peter L. Michaelson, Esq.
(732)530-6671

【File name】 Application
【Kind of Right】 Patent
【Receiving Office】 Commissioner of the Korean Industrial Property Office
【Filing Date】 November 20, 2000
【Title】 METHOD OF PROVIDING TIME STAMPING SERVICE FOR SETTING CLIENT'S SYSTEM CLOCK
【formerly English Title】 A NEW TIME STAMPING SERVICE FOR SETTING CLIENT'S SYSTEM CLOCK

【Applicant】
【Name】 Korea Telecom
【Code】 2-1998-005456-3
【Attorney】
【Name】 Young-Sun Park
【Code】 9-1998-000224-1

【Inventor(s)】
【Name】 Young-Sook LIM
【Name】 Kyung Hee KANG
【Name】 Seung-Jae LEE

【The ground】 The above patent application is hereby made pursuant to Article 42 of the Patent Act.

Attorney(s): Young-Sun Park (Seal)

【Payment】
【Basic fee】 20 sheet(s) 29,000 Won
【Additional fee】 1 sheet(s) 1,000 Won
【Claiming Priority fee】 None
【Fee of request for examination】 6 claims 301,000 Won
【Total fee】 331,000 Won

【Enclosed Documents】 1. 1 set of abstract and specification(drawings)



919980002241



10111010000000000000

방식 심사 란	담 당	심 사 관

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2000.11.20

【발명의 국문명칭】 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑
서비스 방법

【발명의 영문명칭】 A new time stamping service for setting client's
system clock

【출원인】

【명칭】 한국전기통신공사

【출원인코드】 2-1998-005456-3

【대리인】

【성명】 박영순

【대리인코드】 9-1998-000224-1

【포괄위임등록번호】 1999-068257-0

【발명자】

【성명의 국문표기】 임영숙

【성명의 영문표기】 LIM, YOUNG SOOK

【주민등록번호】 650313-2730411

【우편번호】 463-070

【주소】 경기도 성남시 분당구 야탑동(장미마을) 코오롱아파트 129-1101

【국적】 KR

【발명자】

【성명의 국문표기】 강경희

【성명의 영문표기】 KANG, KYUNG HEE

【주민등록번호】 680727-2470614

【우편번호】 137-792

【주소】 서울특별시 서초구 우면동 17

【국적】 KR

【발명자】

【성명의 국문표기】 이승재

【성명의 영문표기】 LEE, SEOUNG JAE

【주민등록번호】 621120-1037024

【우편번호】 463-500

【주소】 경기도 성남시 분당구 구미동(무지개마을) 111 그랜드빌 404-101

【국적】 KR

【심사청구】 청구

【조기공개】 신청

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구
, 특허법 제64조의 규정에 의한 출원공개를 신청합니다.

대리인

박영순 (인)

【수수료】

【기본출원료】	20	면	29,000	원
---------	----	---	--------	---

【가산출원료】	1	면	1,000	원
---------	---	---	-------	---

【우선권주장료】	0	건	0	원
----------	---	---	---	---

【심사청구료】	6	항	301,000	원
---------	---	---	---------	---

【합계】			331,000	원
------	--	--	---------	---

【첨부서류】 1. 요약서 · 명세서(도면)_1통

【요약서】

【요약】

본 발명은 가입자 단말의 시스템 시간을 신뢰할 수 있는 표준시간으로 설정하고자 하는 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 방법에 관한 것이다.

본 발명은 공개키 '보안 서비스를 원활히 제공하기 위해서' 전체되는 '조건 중의 하나' 한가 가입자 단말의 시스템 시간이 정확히 설정되어 있는가 하는 것이므로 시간에 대한 객관성을 부여할 수 있는 임의의 시스템으로 시간정보를 입력받아 가입자 단말의 시스템 시간을 설정하고 이를 기반으로 보안 서비스를 제공하며, 타임 스탬프 서버로부터 기준 시간 정보를 안전하게 받아 가입자 단말의 시스템 시간을 설정할 수 있는 메커니즘을 제공하여 가입자 단말의 시스템 시간에 대한 정확성/신뢰성을 부여함은 물론 서비스 제공업자가 원활하게 보안 서비스를 제공할 수 있으며 보안서비스에 대한 가입자들의 상대적인 민원 건수를 줄임으로써 보안 서비스의 질을 향상시킬 수 있도록 한 것이다.

【대표도】

도 2a

【명세서】**【발명의 명칭】**

가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 방법{A new time stamping service for setting client's system clock}

【도면의 간단한 설명】

도 1은 본 발명에 따른 하드웨어 블록도

도 2는 본 발명에 따른 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 처리 절차를 나타낸 플로우차트

도 3은 본 발명에서의 인증서 취소목록의 유효성 검증 절차를 나타낸 플로우차트

〈도면의 주요부분에 대한 부호의 설명〉

1:제1가입자 단말

2:제2가입자 단말

3:TSA

4:디렉토리 서버

5:인터넷

【발명의 상세한 설명】**【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

<8> 본 발명은 정보 보안 분야에 관한 것으로, 특히 공개키 기반의 보안서비스를 제공하려는 서비스 제공업자들이 가입자 단말에 설정되어 있는 시스템 시간 정보에 대한 신뢰성을 부여하기 위해 신뢰할 수 있는 제3자 시스템에게서 기준 시간 정보를 안전하게

전달받아 가입자 단말의 시스템 시간을 재 설정할 수 있도록 하는 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 방법에 관한 것이다.

- <9> 최근 한국통신 등의 통신사에서는 국민연금, 전자처방전 등 EDI서비스 제공시에 PKI 기반의 보안 서비스를 같이 제공하고 있다.
- <10> 그러나 보안 서비스는 인증서 검증을 위해 정확한 시간을 요구하지만 가입자 단말의 시스템 시간 오류로 인해 서비스가 정상적으로 제공되지 않고 수입의 누수 요인으로 작용되고 있다.
- <11> 통상, 타임 스탬핑 서비스의 목적은 일정한 시점에 특정 문서가 존재하였음을 증명하고 그에 따른 시간의 정확성을 보증하는 것이다.
- <12> 따라서, 타임 스탬핑 서비스를 가입자 단말의 시스템 시간 설정에 적용하고자 하는 메커니즘은 관련 문서에 언급되어 있지 않다.
- <13> 또한, 공개키 기반의 보안 서비스처리와 관련하여 인증서 취소목록을 이용한 인증서 유효성 검증을 할 때 그 판단의 기준이 되는 로컬 타임을 어디에서 어떤 방식으로 가져 올지에 대해 정의된 결론이 없는 상태이다.
- <14> 따라서, 일반적으로 가입자가 보안서비스를 사용하는 단말의 시스템 시간을 로컬 타임으로 사용하는데, 이 과정에서 시스템 시간이 부정확함으로 인해 인증서 취소목록이나 인증서 등이 유효함에도 불구하고 보안서비스를 제공할 수 없는 문제가 발생된다.

【발명이 이루고자 하는 기술적 과제】

- <15> 본 발명은 이와 같은 종래의 문제점을 해결하기 위한 것으로, 본 발명의 목

적은, 가입자 단말의 시스템 시간 설정을 위해 기 정의된 타임 스탬프 스펙에 신규 서비스를 추가/정의하고 그에 따른 TimeStampReq, TimeStampResp 메시지 구조를 수정하여, 객관적으로 신뢰할 수 있는 시간정보를 제공해주는 타임스탬프로부터 시간정보를 받아와 가입자의 시스템 시간을 재 설정할 수 있는 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 방법을 제공하는데 있다.

【발명의 구성 및 작용】

<16> 이와 같은 목적을 달성하기 위한 본 발명은, 서비스 요청자(이하 '리퀘스터'라 함)가 타임스탬프 서버에서 타임스탬프 서비스를 요청하는 제 1단계; 타임스탬프 서버가 타임스탬프 서비스 요청을 받고 이에 대한 응답메시지를 생성/전송하는 제 2 단계; 리퀘스터가 응답메시지를 받고 이에 대한 무결성 검증을 수행하는 제 3단계; 디렉토리 서버로부터 인증서 취소 목록을 가져와 이에 대한 유효성 검증을 하는 제 4단계; 디렉토리 서버로부터 타임스탬프 서버의 전자서명용 인증서를 가져와 전자 서명값을 검증하고 그 결과에 따라 가입자 단말의 시스템 시간을 설정하는 제 5 단계로 이루어짐을 특징으로 한다.

<17> 이하, 첨부된 도면을 참조하여 본 발명의 실시 예를 상세히 설명하면 다음과 같다.

<18> 도 1은 본 발명의 하드웨어적인 구성을 나타낸 블록도로, 시간 정보를 요청하는 단말 환경이 PC환경인 제1가입자단말(1)과, 시간 정보를 요청하는 단말 환경이 유닉스(UNIX)환경인 제2가입자단말(2)과, 신뢰할 수 있는 시간 정보를 제공해 주는 서버로 유닉스 기반의 시스템에서 작동하는 TSA(타임 스탬프 서버)(3)와, 공개키 기반 인프라를 구성하는 단위 시스템 중의 하나로 모든 객체들의 인증서와 인증서취소 목록을 관리하는 시스템으로 상기 TSA(3)의 전자 서명용 인증서를 관리하는 디렉토리 서버(4)와, 상기 제1, 제2 가

입자단말(1)(2)과 TSA(3) 및 디렉토리 서버(4)간의 기본 통신망으로, TCP/IP망을 기본으로 하거나 PPP와 같은 전화접속 네트워킹을 근간으로 형성될 수 있는 인터넷(5)을 포함하여 구성된다.

<19> 이와 같은 하드웨어적인 구성 하에서 작동하는 본 발명의 작용을 도 2를 참고로 하여 설명하면 다음과 같다.

<20> 본 발명은 크게 5단계로 이루어진다.

<21> 즉, 리퀘스터가 TSA(3)에서 타임스탬프 서비스를 요청하는 제 1단계, TSA(3)가 타임스탬프 서비스 요청을 받고 이에 대한 응답메시지를 생성/전송하는 제 2 단계, 리퀘스터가 응답메시지를 받고 이에 대한 무결성 검증을 수행하는 제 3단계, 디렉토리 서버(4)로부터 인증서 취소 목록을 가져와 이에 대한 유효성 검증을 하는 제 4단계, 디렉토리 서버(4)로부터 TSA(3)의 전자서명용 인증서를 가져와 전자 서명값을 검증하고 그 결과에 따라 가입자 단말(1)(2)의 시스템 시간을 설정하는 제 5 단계로 이루어진다.1

<22> 제 1단계는 도 2에서 S21-S23까지이다.

<23> 먼저, 임의 크기의 난수를 생성하여 TimeStampReq를 구성하는 nonce값으로 설정한다 (S21).

<24> 다음에 해당 서비스 요구가 가입자 단말의 시스템 시간을 설정하기 위함임을 타임 스탬프 서버에게 알리기 위하여, 본 발명에서 정의한 requestType 변수에 2, 즉 getBaseTime를 설정하고 해당 구조체를 TimeStampReq의 확장 필드(extension field)에 추가한다(S22).

<25> 그리고 TimeStampReq를 구성하는 기타 값들을 채운 후 해당 메시지를 TSA(3)에게 전송한

다(S23).

<26> 제2단계는 도 2에서 S24내지 S28까지이다.

<27> TSA(3)에서 처리하는 일련의 단계를 포함하는데, 먼저 리퀘스터가 보낸 TimeStampReq 메시지를 수신한다(S24).

<28> 그리고 TSA(3)에 수신된 TimeStampReq 메시지에 대한 확인과 검정을 수행한다(S25).

<29> 이 단계에서 에러가 발생하면, TSA(3)는 해당 메시지를 에러 처리하고 그 결과를 리퀘스터에게 전송한 후 해당 프로세스는 종료한다.

<30> 그러나 이 단계가 성공적으로 수행되면 TSA(3)가 응답메시지 즉, TimeStampResp를 구성하는 변수들의 값을 채운다(S26).

<31> 다음에 TSA(3)와 리퀘스터 간의 메시지 무결성을 보장하기 위하여, S26단계에서 생성된 TimeStampResp 구조체로부터 TSTInfo 구조체를 추출하고, 다시 그로부터 추출된 현재시각 정보인 genTime과 리퀘스터가 TimeStampReq 메시지에 실려 보낸 nonce 값을 이용하여 MAC(Message Authentication Code)값을 산출한 후, MAC값 계산 시 이용한 알고리즘 식별자 정보와 MAC값을 본 발명에서 제안하고 있는 MacInfo 구조체의 해당 필드에 각각 설정한다(S27).

<32> 그리고 MacInfo 구조체를 TSTInfo의 확장 필드(extension fields)에 추가하여 본 발명에서 제시한 TimeStampResp 구조체의 생성을 마무리한다.

<33> 이어서, 상기 단계를 거치면서 완성된 응답 메시지 즉, TimeStampResp 메시지를 리퀘스터에게 전송한다(S28).

<34> 제3단계는 도 2에서 S29-S34까지이다.

<35> TSA(3)가 전송한 메시지, 즉 TimeStampResp 메시지를 수신하고(S29), 수신된 응답메시지에 대한 확인 작업을 수행한다(S30).

<36> 이 단계에서 ASN.1 NOTATION 오류와 같은 에러가 발생하면 해당 메시지는 에러 처리된다.

<37> S31 이하는 S30이 성공적으로 수행된 경우에 한하여 수행되는 하위단계들로, TimeStampResp 메시지로부터 TSTInfo 구조체를 추출하고, 메시지 무결성을 체크하기 위해 리퀘스터가 직접 MAC값을 계산한다(S31).

<38> 우선 TSTInfo로부터 genTime 값을 추출하고, 리퀘스터가 생성시켜 타임스탬프 서버에게 보낸 nonce값을 찾아낸다.

<39> 상기 두 변수 값, 즉 genTime 과 nonce값을 이용하여 리퀘스터가 직접 MAC값을 생성한다

<40> 다음에 MAC값을 검증하여 해당 메시지에 대한 무결성이 보장되었는지를 체크한다.

<41> 먼저, 타임스탬프가 보낸 TimeStampResp 메시지로부터 본 발명에서 제시한 MacInfo 구조체를 추출한 후, 다시 그로부터 mac 값을 추출하고, 추출된 mac값과 상기 S31에서 산출한 MAC값이 동일한지를 비교한다(S32).

<42> 만일, 동일하지 않은 경우에는 TSA(3)가 보낸 현재 시각 정보, 즉 genTime이 중간에 변조되었음을 인정하고(S33), 무결성이 보장되지 않았기 때문에 가입자 단말(1)(2)의 시스템 시간을 설정 할 수 없음을 인지하고 그에 따른 오류를 처리한다(S34).

<43> 그러나 상기 S32에서 mac값이 동일한 경우에는 메시지 무결성이 보장되었음을 인정하여 다음의 제4단계를 수행한다.

<44> 제4단계는 도 2에서 S35-S37까지이다.

<45> 먼저, 인증서와 인증서 취소목록(Certificate Revocation List, CRL)을 관리하는 디렉토리 서버(4)로부터 인증서취소목록과 TSA(3)의 전자서명용 인증서를 가져온다(S35).

<46> 그리고 TSA(3)가 응답 메시지를 통해 보내온 genTime을 기준으로, 디렉토리 서버(4)로부터 가져온 인증서취소목록의 유효성을 검증하기 위해 인증서 취소목록으로부터 thisUpdate와 nextUpdate에 설정된 시간 정보를 가져온다(S42).

<47> 다음에 genTime이 thisUpdate와 nextUpdate사이에 포함되는지를 비교하여 해당 인증서취소목록의 유효성을 판단한다(S37).

<48> 이 S37에서 인증서 취소목록이 유효하지 않다는 결론이 나면 해당 인증서취소목록이 유효하지 않기 때문에 TSA(3)가 보낸 서명값(즉, SignerInfo 구조체의 signature value 필드의 값)을 검증할 수 없음을 인지하고(S38), 가입자 단말(1)(2)의 시스템 시간을 설정할 수 없음을 인지하고 그에 따른 에러를 처리한다(S39).

<49> 그러나 상기 S37에서 CRL이 유효하면 제5단계를 수행한다.

<50> 제5단계는 도 2에서 S40-S51까지이다.

<51> 제5단계에서는 TSA(3)가 보낸 서명값 검증을 통하여 최종적으로 해당 genTime을 신뢰할 것인가 말 것인가에 대한 결론을 내린다.

<52> 먼저, TSA(3)의 전자서명용 인증서에 대한 유효성을 검증하기 위해 필요 정보를 추출하고(S40), 추출한 정보들 중, TSA(3)의 인증서 일련번호가 인증서 취소목록에 포함되어 있는가는 체크한다(S41).

<53> 여기서, TSA(3)의 인증서 일련번호가 인증서 취소목록에 포함되어 있는 경우,

TSA(3)가 보내온 서명값을 검증할 수 없게 되므로 가입자 단말(1)(2)의 시스템 시간을 설정할 수 없기 때문에 해당 사항을 에러 처리하게 된다(S42, S43).

<54> TSA(3)의 인증서 일련번호가 인증서취소목록에 포함되지 않은 경우에는 TSA(3)가 보내온 서명값을 검증하기 위한 사전작업을 수행한다.

<55> 즉, 디렉토리 서버(4)에서 가져온 TSA(3)의 전자서명용 인증서에서 공개키를 추출한다.

<56> 그리고 TimeStampResp메시지를 구성하는 SignerInfo 구조체로부터 Signature value를 추출한 후, 공개키를 이용해 복호하고 그에 따른 해쉬값(이하 M1이라 함) 즉, 다이제스트 값을 구한다(S44).

<57> 다음에 리퀘스터가 SignerInfo 구조체에 있는 다이제스트알고리즘(digestAlgorithm)을 이용하여 직접 해쉬값(이하 M2라 함)을 구한다(S45).

<58> 이 상태에서 두개의 해쉬값, 즉 M1, M2가 같은가를 비교하여 M1과 M2가 다른 경우에는 해당 TimeStampResp 메시지는 정당한 타임스탬프 서버가 보낸 것이 아님을 인지하고, 그에 따라 가입자 단말의 시스템 시간을 설정할 수 없음을 인지하고 관련되는 에러 처리를 수행한다(S47, S48).

<59> 그러나 M1=M2인 경우에는 TSA(3)로부터 받은 TimeStampResp 메시지는 정당한 타임스탬프 서버가 보냈음을 인지한다(S49).

<60> 그리고 TimeStampResp로부터 추출한 genTime으로 가입자 단말의 시스템 시간을 설정하며(S50), 이하 연속되는 서비스를 진행한다(S51).

<61> 도 3은 가입자 단말의 시스템 시간이 제대로 설정되지 않았을 때 보안 서비스를 제

공할 수 없게 되는 일련의 과정을 나타낸 플로우차트로, 먼저 디렉토리 서버(4)로부터 CRL을 다운로드받고, CRL을 디코딩한다(S1, S2).

<62> 다음에 CRL로부터 CRL의 유효시간을 추출하고, 가입자 단말로부터 현재시간 즉 Tcurrent를 추출한다(S3, S4).

<63> 그리고 thisUpdate<Tcurrent< nextUpdate을 비교하여 아닐 경우 인증서 유효성 검증에 실패한 것으로 인정되며, 옳을 경우 CRL로부터 revokedCertificates구조체를 추출하고(S7), revokedCertificates에 해당 인증서가 포함되었는가를 판단하여 포함되지 않았으면 해당 인증서가 폐지되었음이 인정되는 한편 포함되었으면 해당 인증서의 유효성이 인정되는 것이다(S8-S10).

【발명의 효과】

<64> 이상에서 설명한 바와 같은 본 발명은 부인봉쇄서비스 제공과 관련하여, 특정 시점에 특정 메시지가 존재하였음을 객관적으로 증명할 수 있도록 리퀘스터에게 신뢰할 수 있는 표준시간 정보를 제공함과 함께 기본적으로 가입자 단말의 시스템 시간을 객관적으로 인정할 수 있는 표준시간으로 설정할 수 있도록 리퀘스터에게 표준시간 정보를 제공할 수 있는 타임스탬핑 서비스를 제공하여 가입자 단말의 시스템 시간 정보에 대한 신뢰성과 객관성을 확보할 수 있다.

<65> 또한, 공개키 기반의 보안 서비스와 관련하여 가입자 단말의 부정확한 시스템 시간 정보로 인한 보안 서비스 장애 요소를 근본적으로 해결할 수 있는 효과가 있다.

【특허청구범위】**【청구항 1】**

리퀘스터가 타임스탬프 서버에서 타임스탬핑 서비스를 요청하는 제 1단계,

타임스탬프 서버가 타임스탬핑 서비스 요청을 받고 이에 대한 응답메시지를 생성/전송하

는 제 2 단계,

리퀘스터가 응답메시지를 받고 이에 대한 무결성 검증을 수행하는 제 3단계,

디렉토리 서버로부터 인증서 취소 목록을 가져와 이에 대한 유효성 검증을 하는 제

4단계,

디렉토리 서버로부터 타임스탬프 서버의 전자서명용 인증서를 가져와 전자 서명값

을 검증하고 그 결과에 따라 가입자 단말의 시스템 시간을 설정하는 제 5 단계로 이루어

짐을 특징으로 하는 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 방법.

【청구항 2】

제 1항에 있어서, 상기 제1단계가,

임의 크기의 난수를 생성하여 TimeStampReq를 구성하는 nonce값으로 설정하는 과

정,

해당 서비스 요구가 가입자 단말의 시스템 시간을 설정하기 위함임을 타임 스탬프 서버

에게 알리기 위하여 requestType 변수에 getBaseTime를 설정하고 해당 구조체를

TimeStampReq의 확장 필드에 추가하는 과정,

상기 TimeStampReq를 구성하는 기타 값들을 채운 후 해당 메시지를 타임스탬프 서버로

전송하는 과정으로 이루어짐을 특징으로 하는 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 방법.

【청구항 3】

제 1항에 있어서, 상기 제2단계가,

리퀘스터가 보낸 TimeStampReq 메시지를 타임스탬프 서버에서 수신하여 수신된

TimeStampReq 메시지에 대한 확인과 검정을 수행하는 과정;

에러 발생시 타임 스탬프 서버는 해당 메시지를 에러 처리하고 그 결과를 리퀘스터에게 전송한 후 해당 프로세스를 종료하는 과정,

성공적으로 수행시 타임 스탬프 서버가 TimeStampResp를 구성하는 변수들의 값을 채우는 과정,

타임 스탬프 서버와 리퀘스터 간의 메시지 무결성을 보장하기 위하여, 상기

TimeStampResp 구조체로부터 TSTInfo 구조체를 추출하고, 추출된 현재시각 정보인

genTime과 리퀘스터가 TimeStampReq 메시지에 실려 보낸 nonce값을 이용하여 MAC값을

산출한 후 MAC값 계산 시 이용한 알고리즘 식별자 정보와 MAC값을 MacInfo 구조체의 해당 필드에 각각 설정하는 과정,

상기 MacInfo 구조체를 TSTInfo의 확장 필드에 추가하여 TimeStampResp 구조체의 생성을 마무리하는 과정,

완성된 응답 메시지인 TimeStampResp 메시지를 리퀘스터에게 전송하는 과정으로 이루어짐을 특징으로 하는 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 방법.

【청구항 4】

제 1항에 있어서, 상기 제3단계가,

타임 스탬프 서버가 전송한 메시지인 TimeStampResp 메시지를 수신하고, 수신된 응답메시지에 대한 확인 작업을 수행하는 과정,

상기 TimeStampResp 메시지로부터 TSTInfo 구조체를 추출하고, 메시지 무결성을 체크하기 위해 리퀘스터가 직접 MAC값을 계산하는 과정,

TSTInfo로부터 genTime 값을 추출하고, 리퀘스터에 의해 생성되어 타임 스탬프 서버로 보낸 nonce값을 찾는 과정,

타임스탬프가 보낸 TimeStampResp 메시지로부터 MacInfo 구조체를 추출하여 그로부터 mac 값을 추출하고, 추출된 mac값과 상기 MAC값이 동일한지를 비교하는 과정,

상기 mac값과 MAC값이 동일하지 않은 경우에는 타임 스탬프 서버가 보낸 현재 시각 정보인 genTime이 중간에 변조되었음을 인정하고, 가입자 단말의 시스템 시간을 설정 할 수 없음을 인지하고 그에 따른 오류를 처리하며, 동일한 경우에는 메시지 무결성이 보장되었음을 인정하는 과정으로 이루어짐을 특징으로 하는 가입자 단말의 시스템 시간 설정을 위한 타임 스탬핑 서비스 방법.

【청구항 5】

제 1항에 있어서, 상기 제4단계가,

인증서와 인증서 취소목록(CRL)을 관리하는 디렉토리 서버로부터 인증서취소목록과 타임 스탬프 서버의 전자서명용 인증서를 가져오는 과정,

타임 스탬프 서버가 응답 메시지를 통해 보내온 genTime을 기준으로 디렉토리 서버로부

터 가져온 인증서취소목록의 유효성을 검증하기 위해 인증서 취소목록으로부터
thisUpdate와 nextUpdate에 설정된 시간 정보를 가져오는 과정

genTime이 thisUpdate와 nextUpdate사이에 포함되는지를 비교하여 해당 인증서취소목록
의 유효성을 판단하여 인증서 취소목록이 유효하지 않다는 결론이 나면 타임 스탬프 서
버가 보낸 서명값을 검증할 수 없음을 인지하고, 가입자 단말의 시스템 시간을 설정-할
수 없음을 인지하여 에러를 처리하는 과정으로 이루어짐을 특징으로 하는 가입자 단말의
시스템 시간 설정을 위한 타임 스탬핑 서비스 방법.

【청구항 6】

제 1항에 있어서, 상기 제5단계가,

타임 스탬프 서버의 전자서명용 인증서에 대한 유효성을 검증하기 위해 필요 정보
를 추출하고, 추출한 정보들 중, 타임 스탬프 서버의 인증서 일련번호가 인증서취소목록
에 포함되어 있는가 체크하는 과정,

상기 타임 스탬프 서버의 인증서 일련번호가 인증서 취소목록에 포함되어 있으면
가입자 단말의 시스템 시간을 설정할 수 없어 해당 사항을 에러 처리하는 과정,

타임 스탬프 서버의 인증서 일련번호가 인증서취소목록에 포함되지 않은 경우에는
디렉토리 서버에서 가져온 타임 스탬프 서버의 전자서명용 인증서에서 공개키를 추출하
는 과정,

TimeStampResp메시지를 구성하는 SignerInfo 구조체로부터 Signature value를 추출
한 후, 공개키를 이용해 복호하여 그에 따른 해쉬값(M1)을 구하고, 리퀘스터가
SignerInfo구조체에 있는 digestAlgorithm을 이용하여 직접 해쉬값(M2)을 구하는 과정,

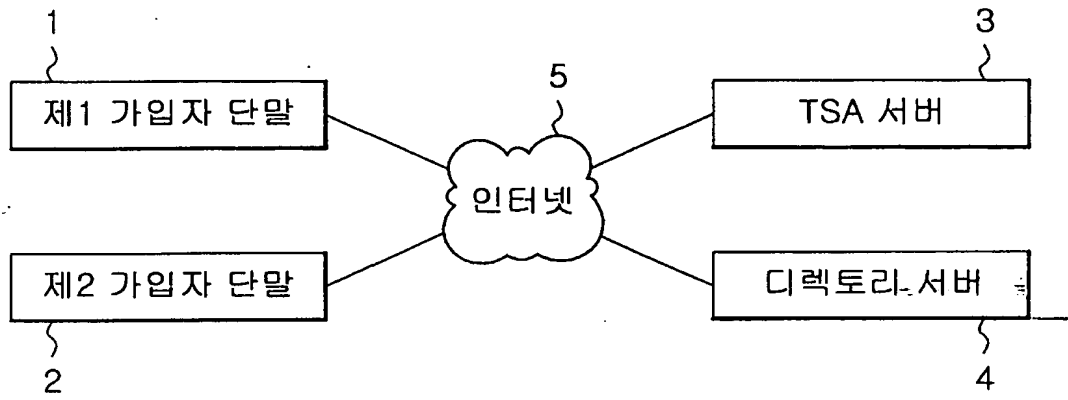
상기 $M1=M2$ 인가를 비교하여 $M1$ 과 $M2$ 가 다른 경우 해당 TimeStampResp 메시지는 정당한 타임 스탬프 서버가 보낸 것이 아니므로 에러 처리를 수행하고, $M1=M2$ 인 경우 TimeStampResp 메시지는 정당한 타임스탬프 서버가 보냈음을 인지하는 과정,

TimeStampResp로부터 추출한 genTime으로 가입자 단말의 시스템 시간을 설정하는

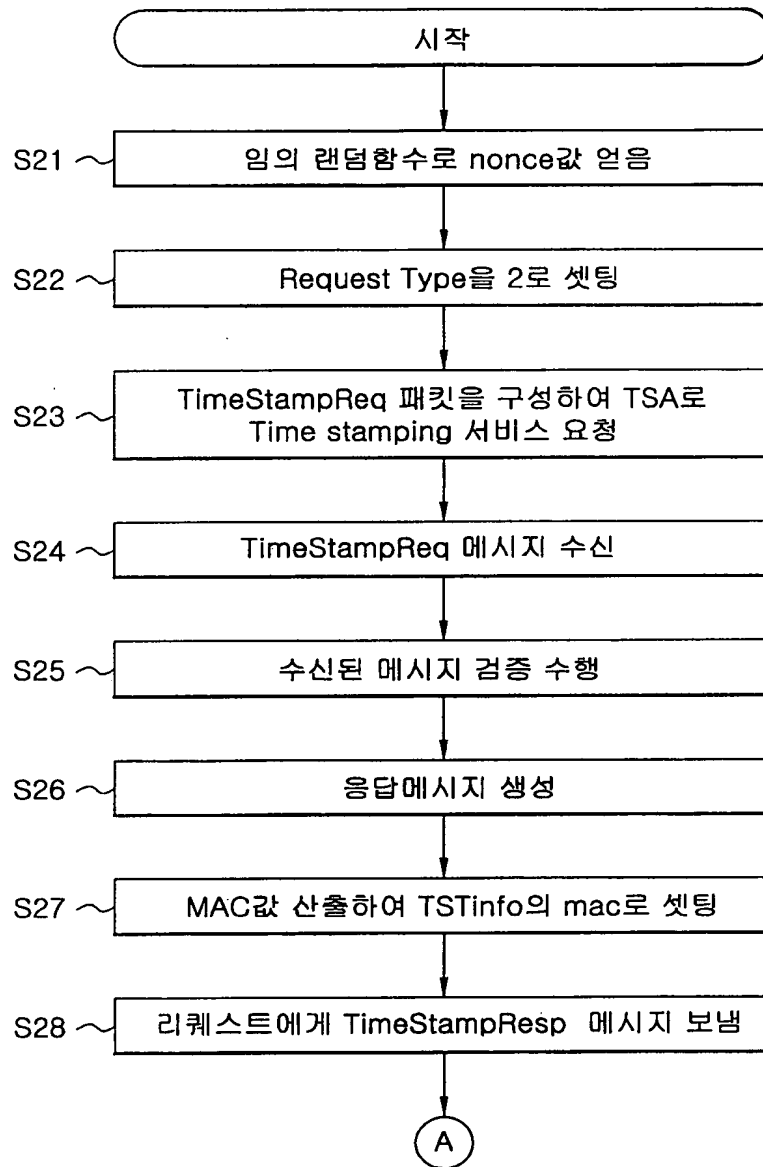
과정으로 이루어짐을 특징으로 하는 가입자 단말의 시스템 시간 설정을 위한 타임 스탬프 서버 서비스 방법.

【도면】

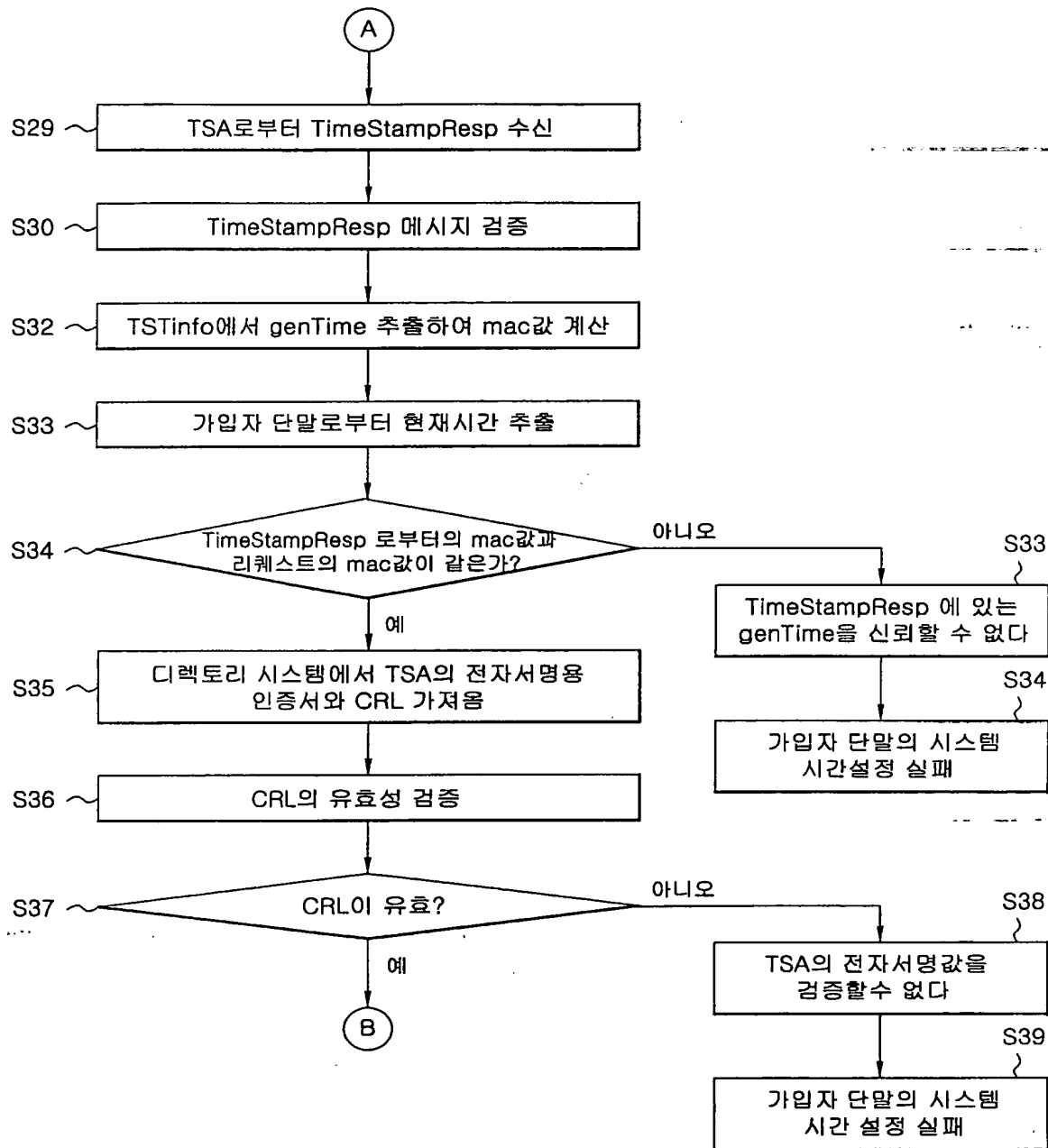
【도 1】



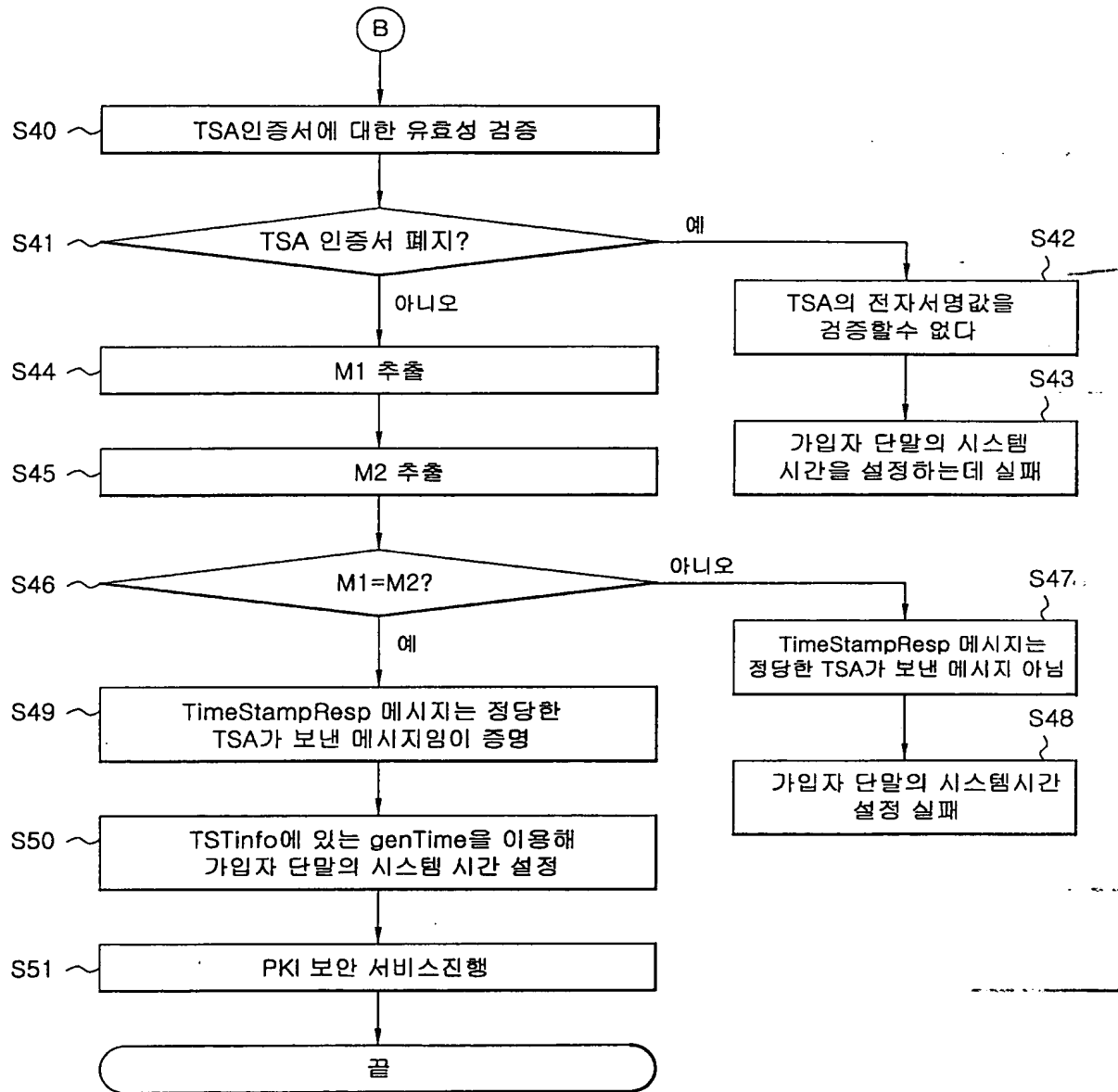
【도 2a】



【도 2b】



【도 2c】



【도 3】

